Q1 Team Name

0 Points

INSYNC

Q2 Commands

10 Points

List the commands used in the game to reach the ciphertext

go, enter, pick, c, c, back, give, back, back, thrnxxtzy, read

Q3 Analysis

50 Points

Give a detailed analysis of how you figured out the password? (Explain in less than 500 words)

Reading the information given on the final screen, we deduced that the problem is of group theory. The password was given to be an element of multiplicative group Z_p^* where p was given to be 455470209427676832372575348833.
This meant that all the group element operations will happen in modulo(p) domain. Further we were provided 3 pairs of numbers of the form $(a, password * g^a)$ which were:
(429, 43195550361823451980800874 9742)
(1973, 176325509039323911968355873643)
(7596, 984869714048619924872947226 13)
Further it was given that the value of g was same for all the pairs.

[+]We tackled this as follows:
Let's consider these 3 integers as a = 429, b = 1973 and c = 7596.
So using this, we formed the following equations:

1) $(pass * g^a) \mod (p) = x$ .....(1)
2) $(pass * g^b) \mod (p) = y$ .....(2)
3) $(pass * g^c) \mod (p) = z$ .....(3)
Now, substituting the value of pass from 1st equation into the 2nd and using modular arithmetic, we got:
$(x * (g^{(b-a)} \mod (p))) \mod (p) = y$ . . . . . $[pass = x * g^{-a} \mod p]$
$(x * x^{-1} * (g^{(b-a)} \mod p)) \mod p = (y * x^{-1}) \mod p$ . . . . . .[Multiplying with x^{-1} on both sides]
=> $g^{(b-a)} \mod p = (y * x^{-1}) \mod p$
=>$g^{1544} \mod p = (y * x^{-1}) \mod p$ .....(5)
Similarly from 2nd and 3rd equations, we get:
=> $g^{(c-b)} \mod p = (z * y^{-1}) \mod p$
=> $g^{5623} \mod p = (z * y^{-1}) \mod p$ .....(6)
Here, b-a = 1544 and c-b = 5623. We observed that GCD(1544,5623) = 1. So, using properties of GCD and bezout's identity, we can find 2 integers u and v such that $1544 * u + 5623 * v = 1$. We got:
$u = -2298, v = 631$

Now using eq. (5) and (6) we calculated g as follows:
$(g^{1544})^u * (g^{5623})^v = ((y * x^{-1})^u * (z * y^{-1})^v) \mod (p)$
..... [multiplying eq. (5) and (6)]

=> $g^{(1544*u+5623*v)} = ((y * x^{-1})^u * (z * y^{-1})^v) \mod (p)$
=> $g^1 = ((y * x^{-1})^u * (z * y^{-1})^v) \mod (p)$
Calculating the inverse of x and y, performing multiplication and after putting the values of u and v, we got:
=> $g^1 = (6367334591911148292811805 2957 * 34726700838987729837401766 7230) \mod (p)$
=> $g = 525650854179633110276943 39$
This value of g matched with the given hint for the value of g. So, we proceeded for getting the password. From eq (1) we can write:
=> $pass = (x * inv(g^a)) \mod (p)$
Substituting this value of g here and finding modulo multiplicative inverse, we finally get the password as:
=> $pass = 13472154209765902984527 3957$

We computed u and v from the following references and wrote the code for performing the modular arithmetic and calculations for

getting the password.
References:
1] https://www.geeksforgeeks.org/bezouts-identity-bezouts-lemma/ (For bezout's identity)
2] https://www.dcode.fr/bezout-identity [Getting coefficients u and v using Extended Euclidian Algo]

Q4 Password

10 Points

What was the final command used to clear this level?

134721542097659029845273957

Q5 Codes

0 Points

Upload any code that you have used to solve this level

compute.py Download

```
1  import math
2  a,x=(429,  431955503618234519808008749742)
3  b,y=(1973, 176325509039323911968355873643)
4  c,z=(7596, 984869714048619924872947226l3)
5
6  p = 455470209427676832372575348833
7  u,v = -2298, 631
8  xinv = pow(x,-1,p)
9  yinv = pow(y,-1,p)
10
11
12 t1 = pow(y*xinv,u,p) # ((x*yinv)**u)%p
13 t2 = pow(z*yinv,v,p)  # ((y*zinv)**v)%p
14 g = pow(t1*t2,1,p)
15 print('g = {}'.format(g),'\nPassword =
   {}'.format((x*pow(g**a,-1,p))%p))
16
```

Assignment 3

GRADED

GROUP

Aman Mittal
Punit Chaudhari
Piyush Gangle
View or edit group

TOTAL POINTS

70 / 70 pts

QUESTION 1

Team Name — **0** / 0 pts

QUESTION 2

Commands — **10** / 10 pts

QUESTION 3

Analysis — **50** / 50 pts

QUESTION 4

Password — **10** / 10 pts

QUESTION 5

Codes — **0** / 0 pts